REMARKS

Claims 1-7, 11-17, 21-27, and 31-39 are pending in the present application. By this response claims 1-7, 11, 14, 17, and 21 are amended, claims 8-10, 18-20, and 28-30 are cancelled, and claims 31-39 are added. Reconsideration of the claims is respectfully requested.

The claims have been amended in order to more clearly recite the invention; these amendments were not made in response to the reference.

I. Interview

The examiner is thanked for the courtesy of the interview held on August 9, 2005. The points discussed in that interview are summarized in the discussion following.

II. 35 U.S.C. § 102, Anticipation: Claims 1-7, 11-17 and 21-27

Claims 1-7, 11-17 and 21-27 stand rejected under 35 U.S.C. § 102(e) as being anticipated by **Molini** et al. (U.S. Patent No. 6,353,385) (hereinafter "**Molini**"). This rejection is respectfully traversed.

Regarding this rejection, the Office Action states:

> Regarding claims 1, 11 and 21, Molini discloses:
>
> logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute (see for example, col. 5, lines 1-10; col. 7, lines 1-6; col. 9, lines 24-29);
>
> classifying events as groups by aggregating events with at least one attribute within the event set as an identical value (see for example, col. 8, lines 25-37; col. 7, lines 19-20; col. 6, lines 49-51; col. 9, lines 30-35);
>
> calculating severity levels for the groups (see, for example, col. 7, lines 50-60; col. 7, lines 27-33);
>
> calculating delta seventies from the severity levels (see, for example, col. 6, lines 52-62; col. 6, lines 15-21, where the highest priority alarm corresponds to the recited delta severity); and
>
> propagating the delta seventies to a higher-level correlation server (see, for example, col. 3, lines 46-59; col. 6, lines 18-37, where the central station corresponds to the recited higher-level correlation server).[1]

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re*

Lowry, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983).

Claim 1 recites that events are logged *in a first correlation server in a hierarchy of correlation servers*, that after *classifying events as groups*, the method then calculates a severity level and delta severity *for each group* and that for each group that has *a non-zero delta severity*, that delta severity is propagated *to a higher-level correlation server*. **Molini** does not anticipate the claimed invention because **Molini** does not show each and every one of these limitations, as will be discussed below.

Representative claim 1 now recites,

> 1. (Amended) A method in a data processing system for reporting security situations, comprising the computer-implemented steps of:
>
> in a first correlation server in a hierarchy of correlation servers, logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute;
>
> classifying events as groups by aggregating events with at least one attribute within the event set as an identical value;
>
> calculating a respective severity level for each of the groups;
> calculating a delta severity for each group from the respective severity level and a respective prior severity level; and
>
> for each group having a non-zero delta severity, propagating the respective delta severity to a higher-level correlation server.

<u>Hierarchy of correlation servers</u>

Claim 1 recites a *first correlation server in a hierarchy of correlation servers*. An exemplary embodiment of such a hierarchy is shown in Figure 10 below, taken from the application as filed. As described in the application on page 17, line 25 through page 19, line 30, correlation servers 1006, 1010, 1014, 1018, and 1022 form a hierarchy. Groups of computers 1000, 1002, and 1004 are monitored by respective correlation servers 1006, 1012, and 1022. Servers 1006 and 1014 collect, analyze, and pass on information regarding their respective computer groups to higher-level server 1010; likewise, servers 1010 and 1022 collect, analyze, and pass on information regarding either the information collected by lower-level server (in 1010) or from a respective group of computers (in 1022) to the top-level server 1018.

[1] Office Action dated June 23, 2005, page 4

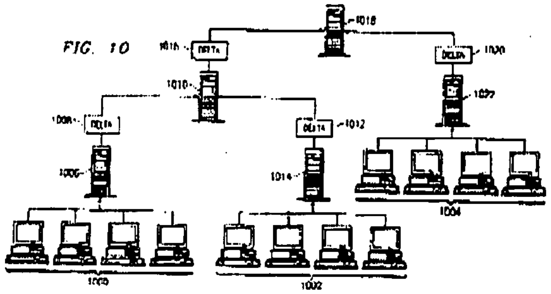

FIG. 10

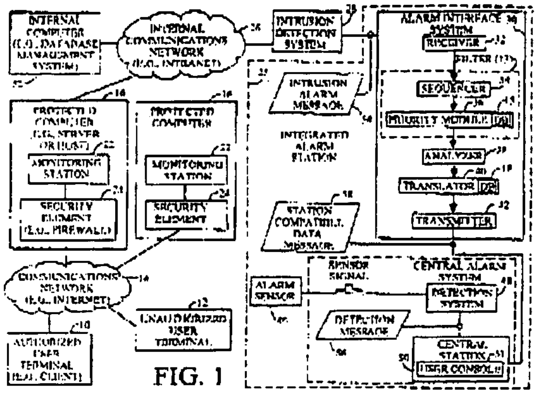

FIG. 1

INTERNAL COMPUTER (E.G. DATABASE MANAGEMENT SYSTEM)
INTERNAL COMMUNICATIONS NETWORK (E.G. INTRANET)
26
INTRUSION DETECTION SYSTEM
28
ALARM INTERFACE SYSTEM 30
RECEIVER
FILTER
SEQUENCER
PRIORITY MODULE
ANALYZER
TRANSLATOR
TRANSMITTER
PROTECTED COMPUTER (E.G. SERVER OR HOST)
PROTECTED COMPUTER
MONITORING STATION
SECURITY ELEMENT (E.G. FIREWALL)
SECURITY ELEMENT
INTRUSION ALARM MESSAGE
INTEGRATED ALARM STATION
STATION COMPATIBLE DATA MESSAGE
COMMUNICATIONS NETWORK (E.G. INTERNET)
UNAUTHORIZED USER TERMINAL
AUTHORIZED USER TERMINAL (E.G. CLIENT)
ALARM SENSOR
SENSOR SIGNAL
CENTRAL ALARM SYSTEM
DETECTION SYSTEM
DETECTION MESSAGE
CENTRAL STATION
USER CONSOLE
10
12
14
16
22
24
32
34
36
38
40
42
48
50
52
54

In contrast, **Molini**, an exemplary embodiment of which is illustrated in Figure 1 above, protected computers 16, are monitored by a single intrusion system 28, which then passes the information to the central alarm system for presentation. **Molini** lacks the advantage of the scalability of the presently claimed invention, but more importantly in the present rejection, **Molini** does not show a *first correlation server in a hierarchy of correlation servers*. Thus, this limitation is not met.

<u>Classifying events into groups</u>

The rejection asserts that the limitation, *classifying events as groups by aggregating events with at least one attribute within the event set as an identical value* is shown by the following excerpts from **Molini**. After each excerpt, a short response to the excerpt is given:

> The priority scheme evaluates incoming data messages according to several criteria to assign a priority level or to filter the incoming data message. After limiting the incoming messages to a time window or sequential group, the priority module **36** evaluates each alarm message according to one or more of the following criteria: (1) a confidence level in the detection of the alarm and (2) a danger posed by an identified attack. The confidence level is evaluated according to confidence factors. Confidence factors may include past experience with a particular alarm type of intrusion alarm messages **28**, the number or percentage of false alarms generated for a particular intrusion alarm messages **28**, a quantitative assessment of specific evaluative criteria used to generate the intrusion alarm messages **28**, and a qualitative assessment of specific evaluative criteria used to generate the intrusion alarm messages **28**. In one example, the confidence level reflects statistical analysis of the processing of historic incoming alarms or intrusion alarm messages. In another example, the confidence level reflects an empirical analysis of historic incoming alarms.[2]

[2] **Molini**, Col. 7, lines 7-26

This excerpt from **Molini** is evaluating individual alarm messages, grouped by time. It does not disclose aggregating the alarms according to the value of their attributes.

> The priority module **36** of the alarm interface system **30** filters the intrusion alarm messages **54** so that the central alarm system **44** and the attending operator are not overwhelmed by a large volume of insignificant alarms. In the context of UL-listed central alarm systems, a central alarm system is required to assure reliable alarm delivery and presentation to an operator by appropriate software instructions or otherwise. For the present central alarm system **44**, the priority module **36** eliminates likely false alarms or an iterative sequence alarms to foster compliance with UL-listing standards for central alarm systems. In certain cases, for example, a single attack may be conducted against as many as 65,536 different ports, causing up to 65,536 separate intrusion alert messages for the same attack.[3]

This excerpt recognizes that a large number of alarm messages can originate from a single attack, but this does not show aggregating the alarms by attribute values.

> The analyzer 38 analyzes the intrusion alarm messages 54 provided by the intrusion detection system 28 to determine characteristics of the attack or unauthorized intrusion upon the protected computer 16. The locale of the attack is one example of a characteristic of the attack or unauthorized intrusion. The intrusion alarm message **54** may define the locale in terms of a source indicator (e.g., source address), a destination indicator (e.g., destination address), or both. The attack of an unauthorized user terminal **12** originates at a source address. The monitoring station **22** may typically detect the attack at or near the destination address of the attack.[4]

This excerpt recognizes that alarm messages have attributes, such as source or destination, but this is not aggregating the alarms by attribute values.

> The database **18** contains relationships among zone identifiers of attacks, destination indicators (e.g., destination addresses) of electronic attacks or security events, and source indicators (e.g., source addresses) of attacks or security events. An intrusion alarm message **54** may contain a destination indicator, a source indicator, or both. A database **18** may contain a mapping of relationships between one or more of the following: (1) a combination of a destination indicator and an origin indicator associated with a corresponding zone, (2) a destination indicator (of an electronic attack or security event) associated with a corresponding zone, and (3) an origin indicator (of an electronic attack or security event) associated with a corresponding zone.[5]

[3] **Molini**, Col. 6, lines 38-51

[4] **Molini**, Col. 8, lines 25-37

[5] **Molini**, Col. 9, lines 24-36

This excerpt discloses how different mappings can be used between the alarm attributes and the zones of a central alarm system having a limited (e.g. 64) number of zones. However, this is not aggregating the alarms by attribute values.

None of the excerpts from **Molini**, either singly or in combination, teach the step of *classifying events as groups by aggregating events with at least one attribute within the event set as an identical value*. Since this step is not anticipated, the claim is allowable.

Severity delta for each group

The rejection asserts that the step of *calculating delta severities*, which has now been amended to recite *calculating a delta severity for each group from the respective severity level and a respective prior severity level* is shown by the following excerpts from **Molini**:

> The sequencer **34** evaluates the incoming data messages within a window of time to define a sequential group of data messages. Similarly, the priority module **36** evaluates the priority within each sequential group. The window may be determined based on the time of receipt of the incoming data messages arrive at the receiver **32**. In one embodiment, the console operator may specify a window of varying duration on a per-system basis. The time window prevents the alarm interface system **30** from waiting for an indeterminate time, expecting a new message to appear from the intrusion detection system **28**. In practice, the alarm interface system **30** operates on a series of successive windows. [6]

In this excerpt, **Molini** is evaluating a group of alarm messages to evaluate the priority within that group. However, this excerpt is not calculating *a delta severity* (i.e., change) between *the respective severity level and a respective prior severity level.* This excerpt is not determining a *delta severity*, nor is it acting on a group that shares attribute values. The use of a delta severity is distinct because it highlights the changes in alarm severity and does not require the transmission of information when groups are unchanging.

> A priority module **36** reviews the alarms in each sequential group. The priority module **36** selects a highest priority alarm within the sequential group. In an alternate embodiment, the priority module **36** reviews the sequential group of alarms and selects a subgroup of highest priority alarms to be transmitted. [7]

Molini is selecting one or a few alarms for transmittal to the central alarm; this excerpt is not determining a delta severity, nor is it acting on a group that share attribute values.

[6] **Molini**, Col. 6, lines 52-63

[7] **Molini**, Col. 6, lines 15-21

None of the excerpts from **Molini**, either singly or in combination, teach the step of *calculating a delta severity for each group from the respective severity level and a respective prior severity level.* Since this step is not anticipated, the claim is allowable.

Propagating severity levels

The rejection asserts that the recitation of *propagating the delta severities*, which has now been amended to recite *for each group having a non-zero delta severity, propagating the respective delta severity to a higher-level correlation server*, is shown by the following excerpts:

> Monitoring stations **22** are associated with corresponding protected computers **16**. The monitoring station **22** refers to a monitoring software program resident in the protected computer **16**, monitoring hardware affiliated with a corresponding protected computer **16**, or both software and hardware. The intrusion detection system **28** communicates to one or more monitoring stations **22** via the internal communications network 14 to determine if unauthorized activity is present. For example, the intrusion detection system **28** may receive data packets or data blocks transmitted from one or more monitoring stations 22. The data packets or blocks may contain data on unauthorized activity, such as attempts of the unauthorized user terminal **12** to access one or more protected computers **16**. In one example, the intrusion detection system **28** polls the monitoring stations **22** for alarm data via the internal communications network 14. In another example, the monitoring stations **22** transmit alarm data on a contention basis or as alarms are detected.
>
> The intrusion detection system **28** is coupled to the alarm interface system **30** of the integrated alarm station 25. The integrated alarm station 25 includes an alarm interface system **30** coupled to a central alarm system **44**. In practice, the alarm interface system **30** and the central alarm system **44** may be co-located at a single site.[8]

> A priority module **36** reviews the alarms in each sequential group. The priority module **36** selects a highest priority alarm within the sequential group. In an alternate embodiment, the priority module **36** reviews the sequential group of alarms and selects a subgroup of highest priority alarms to be transmitted.
>
> Because the alarm interface system **30** accomplishes filtering through the priority module **36**, the number of intrusion alarm messages **54** generated by the intrusion detection system 28 may greatly exceed the number of central station-compatible data messages **58** outputted from the alarm interface system **30** to the central alarm system **44**. The sequencer 34 and the priority module **36** form a filter **13** for filtering incoming data messages. The filter **13** blocks or deletes certain incoming data messages from subsequent transmission via the transmitter **42** to prevent overwhelming of the central alarm system **44** or the central station **50** with incoming alarm messages. The filter **13** preferably has a filtering capacity commensurate with the alarm generating capacity of the

[8] **Molini**, Col. 3, lines 41-65

> intrusion detection system **28**. For example, in certain cases, the intrusion detection system **28** may generate thousands of alarms in a single hour. [9]

These excerpts of **Molini** are not concerned with *delta severities*, nor do they show propagating the *delta severities* to a *higher-level correlation server*. Rather, they send the alarm(s) and their attendant severity levels to a central alarm system. Although the rejection has read the central alarm system on the ***higher-level correlation server***, one of ordinary skill in the art would not see these as the same thing.

None of the excerpts from **Molini**, either singly or in combination, teach the step of, *for each group having a non-zero delta severity, propagating the respective delta severity to a higher-level correlation server*. Since this step is not anticipated, the claim is allowable.

For all the reasons discussed above, claim 1 is not anticipated by **Molini**; therefore this claim is allowable. Further, claims 11 and 21 have been rejected for the same reasons as claim 1; therefore these claims are also allowable.

Dependent claims

Since claims 2-7, 12-17, and 22-27 depend from claims 1, 11, and 21 respectively, the same distinctions between **Molini** and the claimed invention that were argued in claim 1 for these claims is also valid for these dependent claims. The dependent claims recite additional features not taught by the cited reference.

For example, dependent claims 7, 17, and 27 recite an additional combination of features not taught by the reference, specifically, this claim recites *aggregating a subset of the groups into a combined group*.

The rejection of claim 7 asserts:

> Regarding claims 7, 17 and 27, Molini discloses:
> The method of claim 1, further comprising: aggregating a subset of the groups into a combined group (see, for example, col. 9, lines 30-36).

Molini itself states:

> The database **18** contains relationships among zone identifiers of attacks, destination indicators (e.g., destination addresses) of electronic attacks or security events, and source indicators (e.g., source addresses) of attacks or security events. An intrusion alarm message **54** may contain a destination indicator, a source indicator, or both. A database **18** may contain a mapping of relationships between one or more of the following: (1) a combination of a destination indicator and an origin indicator associated

[9] **Molini**, Col. 6, lines 16-37

> with a corresponding zone, (2) a destination indicator (of an electronic attack or security event) associated with a corresponding zone, and (3) an origin indicator (of an electronic attack or security event) associated with a corresponding zone.[10]

This excerpt is discussing possible mappings between the incoming information and the central alarm system, which has a finite, small number of zones. This has nothing to do with combining subsets of the groups into a combined group, as recited in claims 7, 17, and 27.

Therefore, the rejection of claims 1-7, 11-17 and 21-27 under 35 U.S.C. § 102(e) has been overcome.

Furthermore, **Molini** does not teach, suggest, or give any incentive to make the needed changes to reach the presently claimed invention. **Molini** teaches selecting one or a few high priority alarms for presentation to the operator rather than correlating the large amounts of information into a compact, but comprehensive display of numerous conditions. Absent the examiner pointing out some teaching or incentive to implement aggregation of information and the calculation of delta severities in **Molini**, one of ordinary skill in the art would not be led to modify **Molini** to reach the present invention when the reference is examined as a whole. Absent some teaching, suggestion, or incentive to modify **Molini** in this manner, the presently claimed invention can be reached only through an improper use of hindsight using the applicants' disclosure as a template to make the necessary changes to reach the claimed invĉntion.

III. New Claims

Newly added claims 31-39 correspond to cancelled claims 8-10, 18-20, and 28-30, although they are now dependent on respective ones of independent claims 1, 11, and 21. Dependent claims 8, 18, and 28 each recite additional steps or instructions that continue the process recited in their respective independent claims at the higher-order correlation server. Representative claim 31 recites,

> 31. (New) The method of claim 1, further comprising:
> receiving, in the higher-level correlation server, a plurality of delta packets from a plurality of lower-level correlation servers that include the first correlation server, wherein each delta packet contains the respective delta severity for each group of the respective lower-level correlation server that has a non-zero delta severity;

[10] **Molini**, Col. 9, lines 24-36

performing a first mathematical operation on the plurality of delta packets to form a new delta packet;

if the higher-level correlation server is the top level of the hierarchy of correlation servers, performing a second mathematical operation on the new delta packet and a stored severity packet to form a new severity packet; and

if the higher-level correlation server is not the top level of the hierarchy of correlation servers, propagating the new delta packet to a higher-level correlation server.

Molini does not disclose passing delta packets up a hierarchy of correlation servers; it only shows passing alarms to a central alarm system. Thus, **Molini** does not show the steps of *receiving, in the higher-level correlation server, a plurality of delta packets from a plurality of lower-level correlation servers*. **Molini** discloses that the alarm system can receive one or a group of alarm messages, but it is not receiving delta packets, nor is it performing mathematical operations on the delta packets to create a new delta packet. Finally, **Molini** is not showing that the new delta packet can be passed even further up the hierarchy of correlation servers. Thus, the steps of this claim and the related claims are not shown. These claims are also allowable.

IV. Conclusion

It is respectfully urged that the subject application is patentable over **Molini** and is now in condition for allowance.

The examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: August 16, 2005

Respectfully submitted,

Betty Formby

Betty Formby
Reg. No. 36,536
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Agent for Applicants